IPA 対策のしおり シリーズ（11）

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター

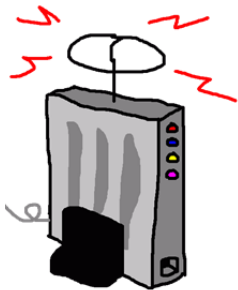
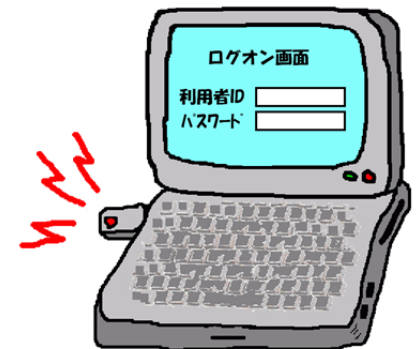
http://www.ipa.go.jp/security/

2015年1月8日 第1.1版

目次

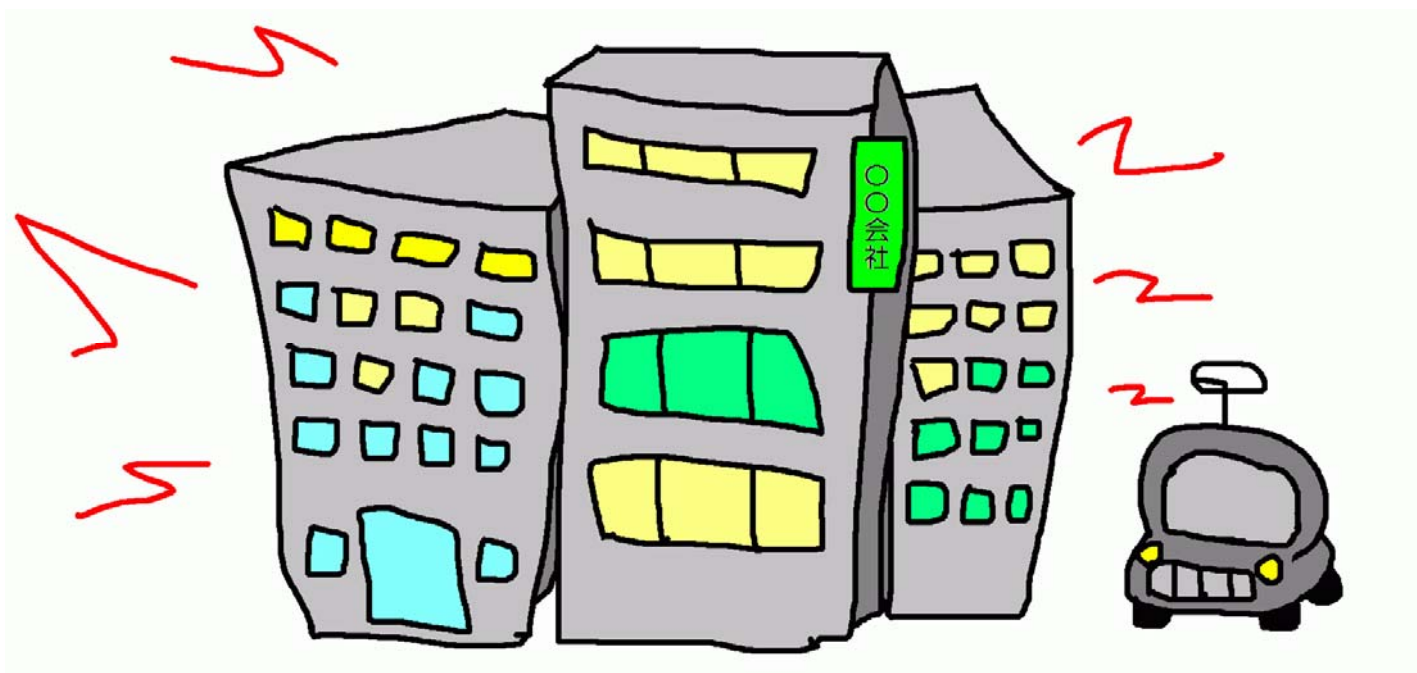
はじめに

企業・組織あるいは一般家庭において、ケーブルを必要としない無線LANは設置が簡単で見栄えが良く、環境構築コストや維持コストが削減できるため、利用者が増加しています。

また、デスクトップパソコンからノートブック等のポータブルデバイスへ移行され始めており、さらに最近のタブレット端末やスマートフォンの接続も簡単にでき、多種多様なデバイスに対応できることから、ケーブル常設の通信経路よりも無線LANの方が利用しやすい状況になっています。さらに無線LANに対応した印刷装置（コピー複合機等）やネットワーク接続ストレージ(NAS)機器も増加傾向です。

こういった背景の中、利用者の増加に伴い、安易な管理・設定・利用からセキュリティ面で問題が発生するケースもあります。

例えば、無線LANの電波の届く範囲が目に見えないため、誰が接続しているのかわからないといった問題…場合によっては、企業・組織や家庭と関係ない人まで接続でき、ただで外部ネットワーク（インターネット）に接続できたり、同じネットワーク上にあるいろいろな情報が抜き取られたりする問題(危険性)…もあるわけです。

実際に無線LANのアクセスポイントに接続していない状態でも、通信自体が暗号化されていない場合は、専用の機器（受信機）を使うことで通信内容を傍受（盗聴）することもできるわけで、これでは仕事上の秘密や個人のプライバシーなどないと言っても過言ではありません。

こういったセキュリティ上の問題(危険)を回避するために、無線 LAN 環境のセキュリティ対策が重要となるわけです。

ウォードライビングという言葉をご存知ですか？

ウォードライビング
　無線 LAN の電波を検知する機器を自動車に積み込み、不正利用可能な無線 LAN のアクセスポイントを求めてオフィス街を走り回ること。アクセスポイントが、脆弱な暗号化通信を行っていたり、推測しやすい接続のためのパスフレーズを使っていたりした場合、それを破り接続することができてしまう。

　IPA が発信する「ニューヨークだより」においても、最近発生しているサイバー攻撃のための情報収集にウォードライビングが利用されていることが紹介されています。興味のある方は以下の資料もご覧ください。

ニューヨークだより 2013 年 4 月
米国におけるサイバーセキュリティ政策の最近の動向
http://www.ipa.go.jp/files/000026543.pdf

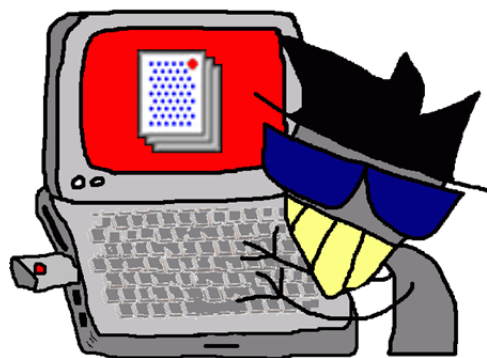
1. どんなリスクがあるのだろう

では、現状ではどんなリスクがあるのでしょうか…

情報セキュリティに弱い企業の場合

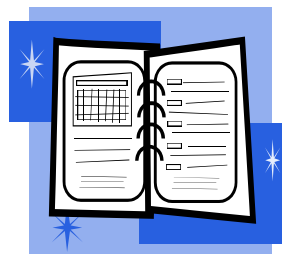
経費削減やさまざまな情報端末に対応できるようなIT環境向上を目的に、安易に無線LANを設置し、管理もせずに運用すると次のようなリスクが発生する可能性があります。

- 無線 LAN への接続認証が不要な設定（つまり暗号化通信を利用しない）や、認証のためのパスフレーズが推測されやすい設定だったりすると、企業・組織の無線LAN環境を企業・組織に無関係な人に利用されることがあります
- 無線 LAN への接続認証が不要な設定（暗号化通信を利用しない）にしていると、電波で飛び交う通信を、無線LANに接続されていなくとも専用の機器を利用して傍受されて、メールが読まれたり、印刷内容が抜き取られること等があります
- 無線 LAN に接続した第三者により、企業・組織のネットワーク上のファイルサーバ、コピー複合機、従業者のパソコン等に保管された顧客情報や従業者の個人情報、営業秘密等の大事な情報を見られたり、抜き取られたり、改ざん・削除されることもあります。
- 話は飛躍しますが、無線LANに慣れてしまった従業者が、無線 LAN の使えるデバイスを企業・組織の外に持ち出し安易に街中の無線LANに接続することもありますが、公衆無線LANは社内の無線 LAN とは環境が違うことを認識していないと…厄介ことになる危険性があります
→「3.企業内で使うノートブックパソコンなどを外部に持ち出した場合の注意事項」をご覧ください

- 等々

一般家庭の場合(参考までに)

利用するデバイスの種類が増えたので、安易に無線LANを設置し、管理もせずに運用すると次のようなリスクが発生する可能性があります。

- 子供がオンラインゲームをするために、友達みんなが無線LANを使えるように認証が不要な設定(暗号化しない状態)にすると、無関係な人まで無線LANが使えるようになります
- 暗号化通信のための認証用のパスフレーズ、買ったままの無線 LAN 機器に貼りついていませんか？パスフレーズをそのまま使っているならば、それを見た人は無線 LAN に無許可で接続できたりします

- 無線 LAN に接続した第三者により、家庭内で共有していた情報(共有ファイル等)を見られる(抜き取られる・改ざんされる・削除される)こともあります
- 設定をセキュリティが弱い方向に設定する(例えばプライバシーセパレータ機能*[1]を止める等)と、どんなWebサイトを参照しているかが、同じ無線 LAN に接続している人に筒抜けになったりします。さらに、悪意のある人が接続していた場合は、プリンターへの印刷内容が抜き取られたり、通信を暗号化していないメールを使用しているとメール本文が読まれたりするだけでなくPOP3*[2]メールのサーバ接続パスワードが盗み見られたりします
- 第三者によって家族になりすまして、外部サイトへ「爆破予告」や「殺人予告」のような危険な書き込みが行われ、場合によっては家族が誤認逮捕されるかもしれません…
- 等々

*1)プライバシーセパレータ機能
　同一の無線 LAN に接続されたデバイス同士の通信を抑制する機能。

*2)POP3
　電子メールのサーバから利用デバイスへの通信に使われる通信方式(プロトコル)。通信が確立されると一方的にメール内容を送り付けるもので、接続のために認証パスワードさえも平文で通信される。

2. 企業内で無線 LAN を使用する際の注意事項

企業内で設備の更新をする際に、企業内ネットワークに無線 LAN を利用する場合があります。利点はネットワーク用にケーブルを引き回す必要がないことが挙げられます。

例えば無線 LAN を利用することで、外部の人も入室可能な会議室でも、必要な人だけがネットワークに接続できる環境を簡単に構築できます。

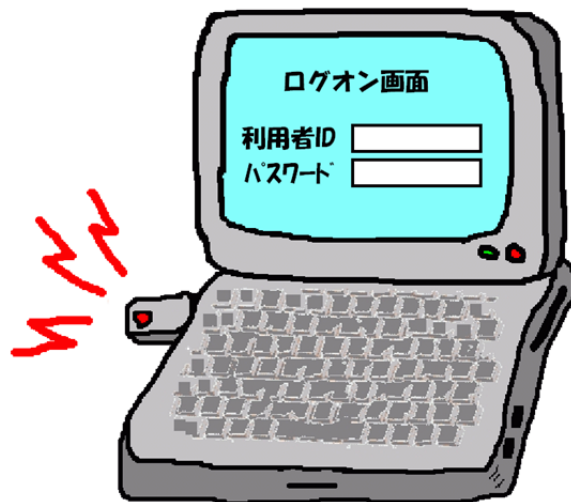
ところが、設定を誤ると誰でも接続できたり、接続方法(例えば認証のためのパスフレーズ)を安易に公開すると接続機器(デバイス)に記憶されたり、それ以降いつでもその機器なら接続できてしまうなどのセキュリティ上の問題を作りこみやすいことも考慮すべきです。

☑ **企業内で無線 LAN を使用する際の注意事項**

- **基本的には無線 LAN 機器の説明書を頼りに、一番セキュリティが強固な使い方(現状では WPA2-PSK による暗号化を利用する)がお勧めですが、設定をセキュリティの弱い方向に変更するとリスクが増加します。無線 LAN でセキュリティ対策を行う理由は二つあります。一つは通信が盗聴されても情報を漏えいさせないことと、第三者が簡単に無線 LAN に接続できないようにするためです**
- **お客様など外部の人がインターネットに接続することを希望した場合、社内のネットワーク接続を許すことはリスクとなります。こういった場合は、社内のネットワークにはつながらない(外部のインターネットにのみ接続できるような)無線 LAN 環境(有線 LAN でも同じですが)を別途用意する必要があります**
- **無線 LAN の接続設定は、一度でも接続を行った場合に接続機器に残るということです(Windows7 以降では、ワイヤレスネットワーク(ネットワーク接続)のプロパティから参照することができます)。お客様だけが利用するような環境であれば定期的接続のためのパスフレーズの変更が有効です**
- **できるなら別途接続のための認証機能を持つ無線 LAN スイッチと認証サーバ等の環境を導入するとセキュリティ対策が向上します**
- **暗号化していれば盗聴や不正使用を防ぐことができるが、それでも電波が企業の外に漏れるのを防ぎたいならば、電波が外に漏れないような物理的対策(たとえば電場遮断シートを窓に貼る)もあります**

3. 企業内で使うノートパソコンなどを外部に持ち出した場合の注意事項

一度無線 LAN の使い勝手に慣れてしまうと、企業の外でもネットワーク接続(無線 LAN)が使いたくなります。以前は、インターネット接続のための専用機器を用意して利用していたネットワーク接続も、最近では街中にサービスとして利用可能な Wi-Fi 接続環境が増えており、専用の通信機器がなくても安易にネットワーク接続することが可能になっています。

こういった環境はスマートフォンに代表されるようなデバイスで効果的に利用されていますが、ノートブックパソコンやタブレットなどでも無線 LAN が使える機器であれば簡単に利用することができます。

当然、企業内で無線 LAN が利用できるようなデバイスであれば、こういった公衆向けの Wi-Fi 環境でネットワーク接続できるので、接続環境について正しい理解を持っていない場合は、セキュリティリスクが増加するので注意が必要です。

したがって、情報機器の持ち出しや持ち出し先での利用方法等についての**従業者教育等**を実施する必要があります。

例えば、以下に示すような項目について、従業者の理解を深めてください。

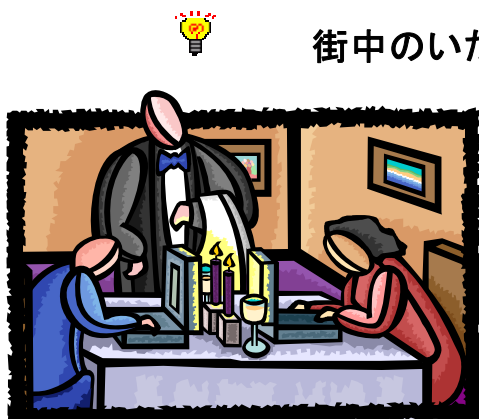
☑ **企業内で無線 LAN を利用するノートパソコンなどを外部に持ち出した場合の注意事項**

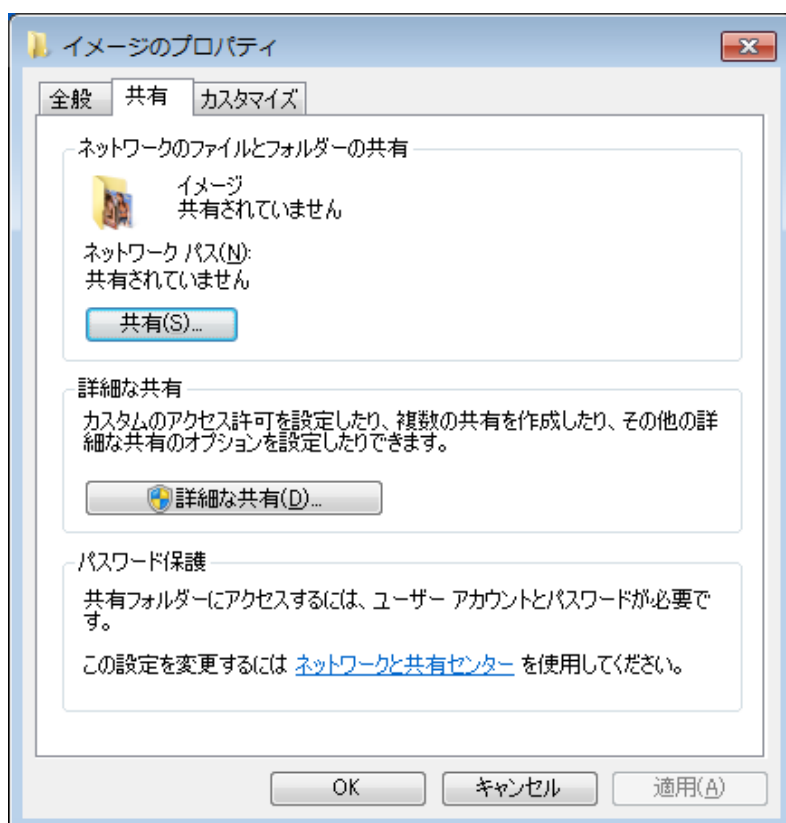
- **公衆向けの無線 LAN（Wi-Fi）環境では、AP（アクセスポイント）管理者や同じ無線 LAN の利用者は信頼できないものとして、無線 LAN を利用すること…常に公の場であることを意識する必要があります!**

- 平文でしか通信できない機能をは使わない(特に利用者 ID やパスワードを平文で通信するような機能は使ってはいけません)。盗聴されればメールの内容は筒抜けです

ログオン画面

利用者ID

パスワード

街中のいたるところで、有償のサービスとして提供されるものだけでなく、個人登録すれば誰でも使えると謳った無線LAN(Wi-Fi)環境が多数利用可能になってきています。利用者は必要に応じてサービスの提供を受けることができますが、そういった無線 LAN 環境の中には、悪意のある利用者あるいは管理者がいる可能性があることを忘れてはなりません

- 公衆の無線 LAN スポットや、ビジネスホテル等での LAN 接続等、不特定多数の利用者が同一 LAN 上に接続する可能性のある環境に接続する場合は、同一 LAN 上の他の利用者から不正アクセスを受ける可能性があります。このような環境では、パソコンの内容がネットワークを通じて第三者に見えるようなフォルダ共有の設定は解除しておく必要があります。

フォルダ共有の設定画面は、当該フォルダの上でマウス「右クリック」→「プロパティ」→「共有」で表示されます。
お使いの OS が Windows 7 の場合は左に示す画面が表示されます。

4. 具体的な対策

前述の注意事項にも記載しましたが、以下に示すような対策を実施することをお勧めします。

- ☑ 用意された最強の暗号化設定（WPA2-PSK）を利用しよう
- ☑ パスフレーズは推測されにくく、ブルートフォース攻撃対策としてある程度の長さ(20 文字以上)が必要
- ☑ さらなるセキュリティ強化を実施するなら、無線 LAN スイッチと認証サーバを利用しよう(多重防御)
- ☑ 万が一の場合に迅速に対応出来るようにするため、ログを収集しておこう
- ☑ 実際の利用者である従業者に対して、新しい環境(無線 LAN 環境)についてのセキュリティリスクの説明や利用基準等を教育しよう
- ☑ 企業内からの無線 LAN 電波の漏れを防ぐなら、無線 LAN 機器の性能を把握し、事務所スペース等に見合った装置を選択するか、電波の漏れない環境を構築しよう

(1)用意された最強の暗号化設定を利用しよう

利用が決まっている無線 LAN 装置(親機)が実装している最強の暗号化設定を利用します。現状では WPA2-PSK となります。暗号化を利用することで次のような効果があります。

- 通信内容が暗号化されるので、物理的に通信が傍受されても通信内容は守られる
- 暗号化をするために必要な認証機能が、無線 LAN の利用者の認証機能（パスフレーズを入力しないと使えない）になる（逆に言えば暗号化しないなら認証もないということです）

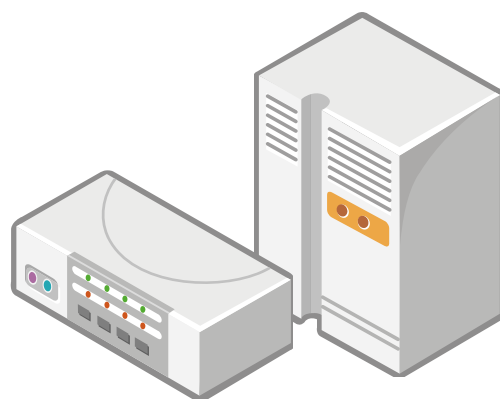
問題となるのは、その設定では利用できない無線 LAN 接続機器（子機ある

いはそういった装置が内蔵された装置類）がある場合は、無理につなげるようにするとセキュリティレベルが下がることを明確にし、そういったセキュリティ面で安全性に欠ける装置は使わないようにすることが重要です（セキュリティ区画を明確に分ける）。セキュリティレベルの一番弱い部分で企業・組織のセキュリティレベルが決まってしまいます。ご注意ください。

(2)パスフレーズは推測されにくく、ブルートフォース攻撃対策としてある程度の長さ(20 文字以上)が必要

力ずくでパスフレーズを破ろうとする攻撃に晒されることを考えるなら、できるだけ桁数の多いパスフレーズを利用すべきです。これらのパスフレーズは通常は利用する機器に一度設定(自動接続設定)したら、パスフレーズを変更しない限り二度と入力することはないと考えていいでしょう。であれば、覚えやすいとか忘れそうもないとか、そういった考慮は不要です。また、無線 LAN 装置(親機)に初期値として設定されているパスフレーズも取扱説明書などが Web で公開されている可能性があるわけで、設定変更した方が良いでしょう。変更したパスフレーズを忘れた場合は、工場出荷状態に戻せば、新たに設定できるはずなので、初期値の情報をなくさなければ、忘れることを心配する必要もないでしょう(機器に貼りつけてあったりしますから)。

(3)さらなるセキュリティ強化を実施するなら、無線 LAN スイッチと認証サーバを利用しよう(多重防御)

大企業などではよく利用されるセキュリティ対策ですが、セキュリティ対策の多重化（多層化）として、複数の無線 LAN 機器を一括管理できるような無線 LAN スイッチと認証サーバを利用するのもよいでしょう。コストパフォーマンスを考慮して利用することになると思われます。

ここで、うんちくを一つ…こんな方法もあり？

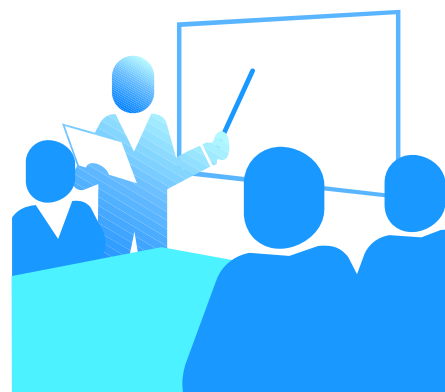
同じような発想から、企業内 VPN 接続を利用する方法（認証サーバを利用する接続方法）もあります。無線 LAN の暗号化通信のための認証と VPN 接続の認証で多重化するもできます。
さらにこんな利用方法も考えられます。
お客様は無線 LAN で外部ネットワークにのみつなげますが、従業者はその無線 LAN を通じて企業・組織内のネットワークにも VPN 接続でつなげるようにできます。これは、いわゆるセキュリティ区画（区画ごとにセキュリティレベルを区分けする）の考え方と同じになりますが、街中の Wi-Fi スポットを企業内に構築するようなイメージになります。この環境では、従業者は街中の無線 LAN を利用するのと同じリスクを伴いますので注意が必要なことは言うまでもありませんが、企業内でも外出先でも同じ使い方ができることになります。

(4)万が一の場合に迅速に対応出来るようにするため、ログを収集しておこう

無線 LAN に限った話ではありませんが、通信の記録を取ることはセキュリティ対策として重要です。何らかの事故（セキュリティ侵害）が起きた場合に調査対象となるだけでなく、平常時の接続監視目的でも利用することができます。
セキュリティ対策としてのログの重要性については、すこし気難しい資料ですが、以下の資料を参考にしてください。

コンピュータセキュリティログ管理ガイド(SP800-92)
米国国立標準技術研究所による勧告
http://www.ipa.go.jp/files/000025363.pdf

(5)実際の利用者である従業者に対して、新しい環境(無線 LAN 環境)についてのセキュリティリスクの説明や利用基準等を教育しよう

無線 LAN に限った話ではありませんが、従業者へのセキュリティ教育は必須です。特に、業務を行う環境や手続きが変更された場合は、新しい環境についてのセキュリティリスクの説明や利用基準等について教育が必要です。

(6)企業内からの無線 LAN 電波の漏れを防ぐなら、無線 LAN 機器の性能を把握し、事務所スペース等に見合った装置を選択するか、電波の漏れない環境を構築しよう

無線 LAN の親機に限らず、企業の事務所(業務)スペース等に見合った機器を利用しよう。あまりに強力な電波を飛ばす機器であれば、業務スペースを超えた場所でも接続情報が知られていれば接続できたり、暗号化されていても通信データが傍受されたりすることがあります。“はじめに”に記述したウォードライビングの話です。こういった問題を防ぐ物理的な対策は、業務スペースに見合った無線 LAN 機器を選定するだけでなく、電波の漏れない環境を作ることができます。

例えば、電波遮蔽シートを窓に貼るのも有効です。

無線 LAN アクセスポイントや無線 LAN クライアントに対しセキュリティ対策を施したとしても、空間を行き交う電波そのものを制限することはできません。これは有線にはない無線特有のものであり、社外に漏れた電波を通じて盗聴、あるいは社内ネットワークに侵入されるおそれがあります。そのため、これほど無線 LAN が普及していない頃には、無線 LAN の導入を躊躇している企業も多かったようです。

利用中の無線 LAN が使用している電波が社外に漏れることを防ぐための対策として、電波遮蔽シートがあげられる。電波遮蔽シートとは、アルミニウムや鉄などの導電体をシート状にしたもので、特に窓などの電波を遮蔽する能力に欠ける箇所に対して設置することが多い。電波遮蔽シートを利用することにより、手軽に窓や壁、天井などに対し電波の漏洩対策を実施することができる。また、遮蔽する周波数帯域を選定できるものもあり、無線 LAN に利用される周波数帯のみを遮蔽し、携帯電話や PHS などのモバイル端末の電波やテレビ電波を通すことができる製品もあるため、無線LAN 機器の選定だけでなく、利用する環境における条件に応じてこういった製品を選択することが重要となります。

5. 参考情報

＜総務省＞

- 企業が安心して無線 LAN を導入・運用するために
  http://www.soumu.go.jp/main_content/000199320.pdf
- 安心して無線 LAN を利用するために
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/lan/pdf/lan_1.pdf

＜社団法人電子情報技術産業協会(JEITA)/経済産業省＞

- 無線 LAN のセキュリティに関する注意事項 第1版
  http://home.jeita.or.jp/page_file/20110510155841_KMAZEPqBFb.pdf

＜明日の暮らしを分かりやすく 政府広報オンライン＞

- これだけはやっておきたい！「無線 LAN 情報セキュリティ 3 つの約束」
  https://www.gov-online.go.jp/useful/article/201303/1.html

＜IPA＞

- 無線 LAN 利用環境のための運用上のセキュリティ対策
  http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/411.html
- 一般家庭における無線 LAN のセキュリティに関する注意
  http://www.ipa.go.jp/security/ciadr/wirelesslan.html
- コンピュータウイルス・不正アクセスの届出状況について
  今月の呼びかけ「無線 LAN を他人に使われないようにしましょう！」
  http://www.ipa.go.jp/security/txt/2011/04outline.html

＜しおり内に掲載した関連情報＞

- ニューヨークだより 2013 年 4 月
  米国におけるサイバーセキュリティ政策の最近の動向
  http://www.ipa.go.jp/files/000026543.pdf

IPA 対策のしおり シリーズ

http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA 対策のしおり シリーズ(1) ウイルス対策のしおり
- IPA 対策のしおり シリーズ(2) スパイウェア対策のしおり
- IPA 対策のしおり シリーズ(3) ボット対策のしおり
- IPA 対策のしおり シリーズ(4) 不正アクセス対策のしおり
- IPA 対策のしおり シリーズ(5) 情報漏えい対策のしおり
- IPA 対策のしおり シリーズ(6) インターネット利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(8) スマートフォンのセキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(9) 初めての情報セキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(10) 標的型攻撃メール 対策のしおり
- IPA 対策のしおり シリーズ(11) 無線 LAN 対策のしおり
- IPA 対策のしおり シリーズ(12) 暗号化による 情報漏えい対策のしおり

IPA 独立行政法人 情報処理推進機構
技術本部 セキュリティセンター

〒113-6591 東京都文京区本駒込2丁目28番8号
（文京グリーンコートセンターオフィス16階）
URL　http://www.ipa.go.jp/security/

【情報セキュリティ安心相談窓口】
URL　http://www.ipa.go.jp/security/anshin/
E-mail　anshin@ipa.go.jp